AO 106 (Rev. 04/10) Application for a Search Warrant

RECEIVED
JAN 10 2019
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND

UNITED STATES DISTRICT COURT

for the

Northern District of California

SEALED BY ORDER OF THE COURT

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

[redacted] Oakland, California [redacted]
including Any Digital Devices Found Therein

REDACTED

Case No. 4-19-70053 KAW

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

[redacted] Oakland, California [redacted] (further described in Attachment A, incorporated by reference)

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B and C, incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875d	Interstate communications (Extortion)

The application is based on these facts:
Please see attached affidavit (incorporated by reference).

[approved as to form AUSA Robert S. Leach Christina McCall for]

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

[redacted]
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

_____
Judge's signature

City and state: Oakland, CA

The Hon. Kandis A. Westmore, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, [redacted], being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Computer Crime Investigative Unit ("CCIU") of the U.S. Army Criminal Investigation Command ("USACIDC"), and have been employed in that position since December, 2013. Prior to that, for approximately five years, I served as a Computer Forensic Examiner with U.S. Army Cyber Command in Fort Belvoir, VA. In addition to my training as a criminal investigator, I have been trained in computer incident response, digital evidence acquisition, and computer forensics at the Department of Defense Cyber Investigations Training Academy in Linthicum, MD, and hold a Master's Degree in Computer Forensics from George Mason University. As a Special Agent of USACIDC, I am authorized to investigate crimes involving violations of the Uniform Code of Military Justice, and other applicable federal laws, where there is an Army interest.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant to search the premises known as [redacted], Oakland, CA [redacted], hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B, as they relate to the violation of 18 U.S.C. § 875, Interstate Communications.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

4. Title 18 U.S.C. § 875d, Interstate communications, states that whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

III. STATEMENT OF PROBABLE CAUSE

Summary

5. US Army CID is currently investigating the extortion of an active duty service member by an unknown individual through Facebook Messenger.

Background to Investigation

6. On December 11, 2017, Special Agent [redacted], Fort Richardson CID Office, Joint Base Elmendorf-Richardson, AK, was notified by Private First Class (PFC) [redacted] that

he was unwilling recorded and being extorted by an unknown individual through Facebook Messenger.

7. On December 10, 2017, [redacted]. Approximately 20 minutes after [redacted], he received a message on Facebook Messenger, in which the sender stated they had a video of [redacted], and that the sender would send the video to all of PFC [redacted]'s Facebook friends and family members if PFC [redacted] did not pay $800.00. PFC [redacted] told the sender that he did not believe the sender. The sender then showed PFC [redacted] the video through Facebook Messenger video chat. PFC [redacted] did not send any funds to the unknown individual and ignored any subsequent communications attempts.

8. On December 11, 2017, PFC [redacted] provided SA [redacted] with his cell phone and signed a Consent to Search for the device.

9. On December 22, 2017, I conducted a forensic review of PFC [redacted]'s cell phone and assessed it was likely there were two Facebook accounts of interest, [redacted] and [redacted], involved in the extortion attempt. I also determined the communications software utilized was Facebook Messenger. I further determined the date of the incident was likely December 10, 2017, with connections at 10:40 and 21:30, Alaska Time Zone; one connection lasted approximately 28.56 minutes which may have been the incident of unwanted recording.

10. On February 22, 2018, SA [redacted], Digital Forensics and Research Branch, CCIU, Quantico, VA, published

Forensic Examination Report [redacted], in which he detailed the results of his examination of PFC [redacted]'s mobile phone. SA [redacted] confirmed Facebook communications between PFC [redacted] and the Facebook accounts [redacted] and [redacted].

11. On January 26, 2018, SA [redacted], CCIU Pacific Office, received subpoena production from Facebook for account information on the Facebook accounts [redacted] and [redacted]. Additionally, SA [redacted] was able to recover messages from the account [redacted] in where the sender was threatening to post the video of PFC [redacted].

a. The account [redacted] was created on December 1, 2017, registered to the name [redacted], and verified with the Mali mobile phone number [redacted].

b. Facebook IP Connection Logs for the account [redacted] showed connections from the IP address [redacted] at the time that PFC [redacted] received messages from the unknown individual. The IP address [redacted] is registered to Aviso (Orange CI), a mobile telephone provider for Ivory Coast, Africa.

c. The Facebook IP Connection Logs for the account [redacted] also showed a login event from the IP address [redacted], also registered to Aviso, on December 13, 2017. Approximately 8 minutes after the connection, the same account logged off of Facebook from the IP address [redacted], which is registered to Comcast Cable Communications.

d. From my training and experience, I know that digital devices can change IP addresses when moved from a mobile telephone wireless network to a wireless network in which they are set to automatically connect. The logs from Facebook are indicative of such a connection.

e. The Facebook account [redacted] was created on November 14, 2017, registered to the name [redacted], and verified with the phone numbers [redacted] (MTN Cote dIvoire (Loteny)) and [redacted] (Orange CI).

f. The Facebook IP Connection Logs for the account [redacted] showed connection events from the same IP addresses at the same times as the activity for the Facebook Account [redacted]. This is indicative that the two Facebook accounts were being controlled by the same physical device and the same individual.

12. On April 6, 2018, SA [redacted] received the subpoena production from Comcast for subscriber information for the IP address [redacted] on December 13, 2017. Comcast records show the IP address was issued to [redacted], OAKLAND, CA [redacted].

13. Research into the name and address provided by Comcast indicated there were two individuals with similar names, having the same address as the Comcast service address. The two individuals, both named [redacted], appear to be father and son. While both of the names had different current addresses listed in their respective Thomson Reuters CLEAR Reports for Law Enforcement and California driver's licenses

(DL), the phone number provided as part of the Comcast subpoena return was tied to both of them. The father, [redacted]'s DL, California [redacted], date of birth [redacted], listed [redacted], Pittsburg, CA [redacted] as a current residence. The son, [redacted]'s DL, California [redacted], date of birth [redacted], had the current address of [redacted], Antioch, CA [redacted] listed. Additionally, there were several vehicles with current vehicle registrations in the name [redacted] and the registration address of [redacted], Oakland, CA [redacted].

14. In summary, I know that devices can change IP addresses when they move within range of a wireless network that they are associated with. For example, when a mobile phone is out of range from a wireless access point, it will use the cellular data network and have an IP associated with the carrier, and when it is returned to the wireless access point coverage, it will automatically connect to the access point, and have an IP associated with the supporting network. I submit that there is probable cause to believe this is the case in this situation. On December 13, 2017, a device connected to the Facebook accounts used to extort PFC [redacted] was initially connected to a foreign based cellular carrier, and then automatically connected to the wireless access point at [redacted], Oakland, CA.

Background on Digital Intrusions

15. From my training and experience, I am familiar with the following terms which are pertinent to this investigation:

a. **IP address:** An Internet Protocol (IP) Address is a unique numeric address used to identify computers on the Internet. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. IP addresses are typically assigned by Internet service providers ("ISP"), such as AOL, Earthlink, Comcast, or cable companies. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection (so-called "dynamic IP addressing"), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called "static IP addressing"). In both scenarios, the IP Address used by a computer attached to the Internet must be unique. ISPs typically log their customers' connections, which means the ISP can identify which of their customers was assigned a specific IP address during a particular session.

b. **Log files.** The term "log files" refers to computer-generated files containing information regarding the activities of computer users, processes running on a computer, and the activity of computer resources. A typical web server log file would contain information about the web site name being requested, if the request was successful, the user's IP address, and the date and time that the request was completed, among other pieces of information. It is frequently also possible for the customer to directly access the server computer through the

Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

c. **Server.** A server is a computer that provides a service for other computers connected to it via a network. When, for example, a user accesses email or an Internet web page, those files are pulled electronically from the server where they are stored and are "served up" or sent to the user's computer via the network or the Internet. Notably, servers can be physically located in any location, for example, it is not uncommon for a network's server to be located hundreds of miles away from the user's computers.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

16. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units;

desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in

the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular

user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal

information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a

controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

17. *Unlocking the device(s) with biometric features.* The search warrant I am applying for would permit law enforcement to

compel certain individuals to unlock a device subject to seizure pursuant to this search warrant using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other

manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition

features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this search warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this search warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some

circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with

certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

i. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this search warrant and may be unlocked using one of the aforementioned biometric features, the search warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face to those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this search warrant.

V. ITEMS TO BE SEIZED

18. Based on the foregoing, I respectfully submit that there is probable cause to believe that the items listed in Attachment B, which constitute evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 875, Interstate communications will be found at the PREMISES. In executing the search warrant, law enforcement agents will comply with the Northern District of California's Protocol for Searching Devices or Media that Store Data Electronically, as set forth in **Attachment C.**

VI. CONCLUSION

19. Based on the foregoing, I request that the Court issue the requested search warrant.

[redacted], Special Agent
U.S. Army Criminal
Investigations Command

Subscribed to and sworn before
me
on January ___, 2019.

THE HONORABLE KANDIS A. WESTMORE
UNITED STATES MAGISTRATE JUDGE

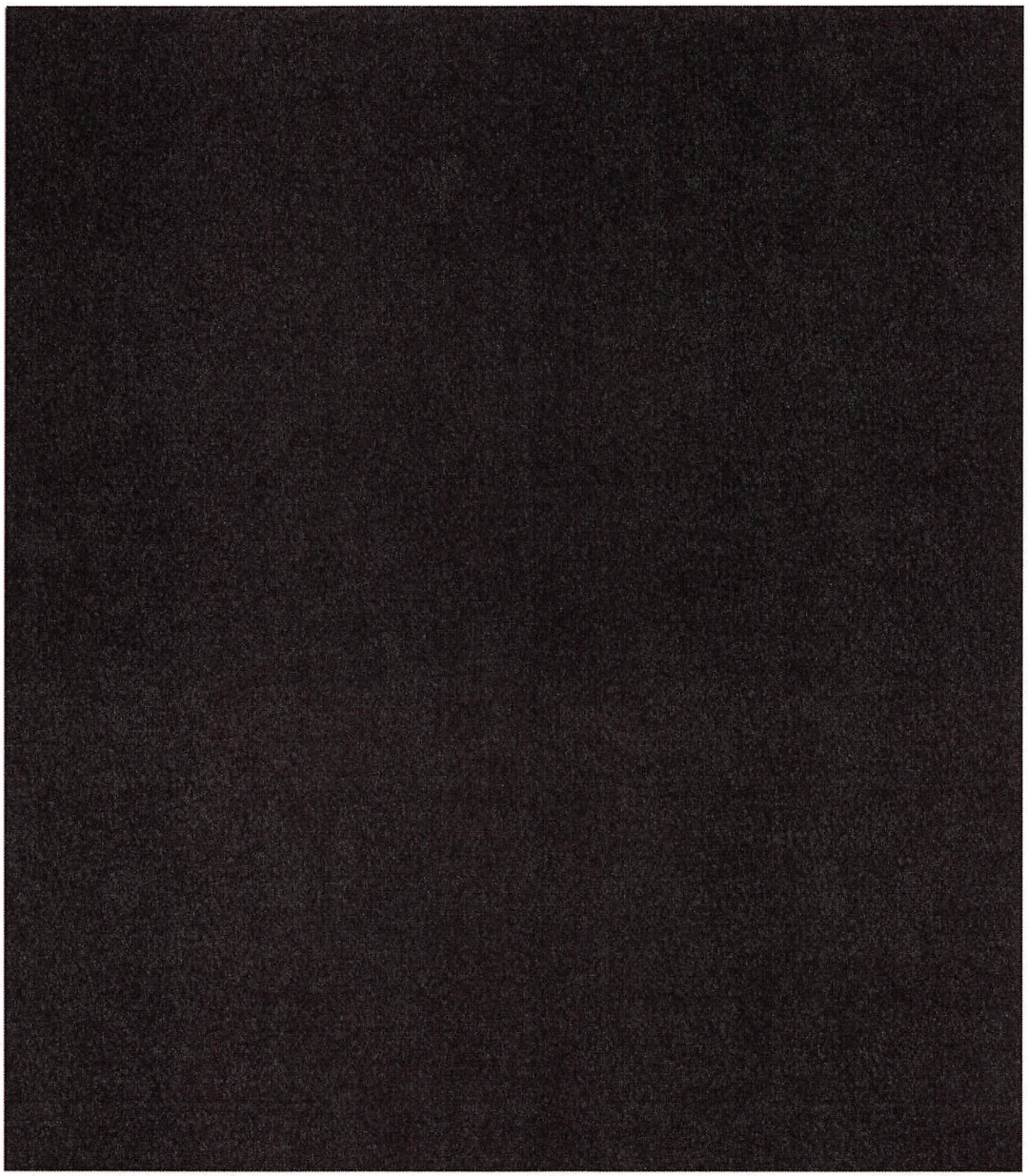
ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to [redacted], Oakland, CA [redacted], hereinafter "PREMISES", further described as [redacted]

[redacted]

[redacted]



The warrant authorizes a search of the PREMISES for the records and information related to the offenses described in Attachment B and seizure thereof and authorizes the subsequent search of any electronic devices seized for records and information related to the offenses described in Attachment B.

This search warrant further authorizes the use of biometric methods as described in Paragraph 17 of the Affidavit in Support of An Application for A Search and Seizure Warrant.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 875, Interstate communications.

2. Records and information related to the identity or location of the person who utilized the IP address [redacted] (SUBJECT IP).

3. Computers or storage media used as a means to commit the violations described above.

4. For any computer or storage medium whose seizure is otherwise authorized by this search and seizure warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this search and seizure warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this search and seizure warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Records and information relating to access to Facebook;

c. Records and information related to the identity or location of the person who utilized the IP address [redacted] (SUBJECT IP);

d. SSH, FTP, or Telnet logs showing connections related to the SUBJECT IP, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;

e. Records of and information about who used, owned, or controlled the SUBJECT IP at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

f. Software that would allow others to control the **COMPUTER**, such as viruses, Trojan horses, and other forms of malicious software; records of or information about such software; and evidence of the presence or absence of security software designed to detect malicious software;

g. Counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT HARD DRIVE; and records of or information about such software;

h. Records of or information about the times the **COMPUTER** was used;

i. Records or information that might identify the persons leasing or operating the **COMPUTER**, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), types of services utilized, means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

j. Contextual information necessary to understand the evidence described in this attachment.

5. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

6. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony

PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

7. During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this search warrant.

ATTACHMENT C

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA
PROTOCOL FOR SEARCHING DEVICES OR MEDIA THAT STORE DATA ELECTRONICALLY

1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.

2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.

3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.

4. When the government removes a device from the searched premises it may also remove any equipment or documents ("related equipment or documents") that reasonably appear to be necessary to create a mirror image of the contents of the device or conduct an off-site forensic review of a device.

5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14 calendar days of the execution of the search warrant.

6. Within a reasonable period of time, but not to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain such data.

7. The time periods set forth in this protocol may be extended by court order for good cause.

8. In the forensic review of any device or image under this warrant the government must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically-stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably

practicable.

9. For the purposes of this search protocol, the phrase "to preserve evidence" is meant to encompass reasonable measures to ensure the integrity of information responsive to the warrant and the methods used to locate same.